

IN THE CLAIMS

Amended claims follow:

1. (Currently Amended) A method for preventing writes to critical files, comprising:
[[[a]]] identifying factors associated with a computer;
[[[b]]] monitoring requests to write to files on the computer; and
[[[c]]] conditionally preventing the writes to the files on the computer based on the factors to prevent virus proliferation;
[[[d]]] wherein the factors are altered based on the monitoring of the requests to write to the files on the computer;
[[[e]]] wherein the factors are updated based on the requests;
wherein if one of the requests is initiated by an application that is not one of a plurality of trusted applications, a user is alerted and allowed to at least one of prevent and permit the request initiated by the application.
2. (Currently Amended) The method as recited in claim 1, wherein the factors are selected from the group consisting of critical files, critical file locations, and the plurality of trusted applications.
3. (Original) The method as recited in claim 1, wherein the factors are user configurable.
4. (Original) The method as recited in claim 1, wherein the factors are identified in a registry.
5. (Original) The method as recited in claim 2, wherein the factors include critical files associated with an operating system of the computer.
6. (Original) The method as recited in claim 2, wherein the factors include critical file locations associated with an operating system of the computer.

7. (Original) The method as recited in claim 6, wherein the critical file locations include folders.
8. (Currently Amended) The method as recited in claim 2, wherein the factors include the plurality of trusted applications that initiate the requests.
9. (Original) The method as recited in claim 1, wherein the factors are updated based on a user request.
10. (Original) The method as recited in claim 1, wherein the factors are updated from a remote location via a network.
11. (Cancelled)
12. (Original) The method as recited in claim 1, and further comprising conditionally preventing the writes to the files on the computer based on a user confirmation.
13. (Original) The method as recited in claim 12, wherein the factors are updated based on the user confirmation.
14. (Currently Amended) A computer program product embodied on a tangible computer readable medium for preventing writes to critical files, comprising:
 - [[[(a)]] computer code for identifying factors associated with a computer;
 - [[[(b)]] computer code for monitoring requests to write to files on the computer, and
 - [[[(c)]] computer code for conditionally preventing the writes to the files on the computer based on the factors to prevent virus proliferation;
 - [[[(d)]] wherein the factors are altered based on the monitoring of the requests to write to the files on the computer;
 - [[[(e)]] wherein the factors are updated based on the requests;

wherein if one of the requests is initiated by an application that is not one of a plurality of trusted applications, a user is alerted and allowed to at least one of prevent and permit the request initiated by the application.

15. (Currently Amended) The computer program product as recited in claim 14, wherein the factors are selected from the group consisting of critical files, critical file locations, and the plurality of trusted applications.

16. (Original) The computer program product as recited in claim 14, wherein the factors are user configurable.

17. (Original) The computer program product as recited in claim 14, wherein the factors are identified in a registry.

18. (Original) The computer program product as recited in claim 15, wherein the factors include critical files associated with an operating system of the computer.

19. (Original) The computer program product as recited in claim 15, wherein the factors include critical file locations associated with an operating system of the computer.

20. (Original) The computer program product as recited in claim 19, wherein the critical file locations include folders.

21. (Currently Amended) The computer program product as recited in claim 15, wherein the factors include the plurality of trusted applications that initiate the requests.

22. (Original) The computer program product as recited in claim 14, wherein the factors are updated based on a user request.

23. (Original) The computer program product as recited in claim 14, wherein the factors are updated from a remote location via a network.

24. (Cancelled)

25. (Original) The computer program product as recited in claim 14, and further comprising computer code for conditionally preventing the writes to the files on the computer based on a user confirmation.

26. (Original) The computer program product as recited in claim 25, wherein the factors are updated based on the user confirmation.

27. (Currently Amended) A system including a tangible computer readable medium for preventing writes to critical files, comprising:

[[(a)]] logic for identifying factors associated with a computer;

[[(b)]] logic for monitoring requests to write to files on the computer; and

[[(c)]] logic for conditionally preventing the writes to the files on the computer based on the factors to prevent virus proliferation;

[[(d)]] wherein the factors are altered based on the monitoring of the requests to write to the files on the computer;

[[(e)]] wherein the factors are updated based on the requests;

wherein if one of the requests is initiated by an application that is not one of a plurality of trusted applications, a user is alerted and allowed to at least one of prevent and permit the request initiated by the application.

28. (Currently Amended) A method for preventing writes to critical files, comprising:

[[(a)]] identifying an operating system associated with a computer;

[[(b)]] looking up at least one of critical files and critical file locations associated with the operating system; and

[[(c)]] preventing access to the at least one of critical files and critical file locations associated with the operating system to prevent virus proliferation;

[(d)] wherein the at least one of critical files and critical file locations are looked up based on requests to write to the at least one of critical files and critical file locations on the computer;

wherein if one of the requests is initiated by an application that is not one of a plurality of trusted applications, a user is alerted and allowed to at least one of prevent and permit the request initiated by the application.

29. (Cancelled)

30. (Previously Presented) The method as recited in claim 1, wherein the factors include a list of critical files such that the list of critical files is updated based on the requests.

31. (Currently Amended) The method as recited in claim 8, A method, comprising:
identifying factors associated with a computer;
monitoring requests to write to files on the computer, and
conditionally preventing the writes to the files on the computer based on the
factors to prevent virus proliferation;
wherein the factors are altered based on the monitoring of the requests to write to
the files on the computer;
wherein the factors are updated based on the requests;
wherein the factors include trusted applications that initiate the requests;
wherein if one of the requests is initiated by an application that is not one of the trusted applications, a user is alerted and allowed to at least one of prevent and permit the request initiated by the application.